Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance	)	CC Docket No. 97-213
For Law Enforcement Act	)	
	)	

COMMENTS OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY

James X. Dempsey, Senior Staff Counsel
Daniel J. Weitzner, Deputy Director
Center for Democracy and Technology
1634 Eye Street, N.W., Suite 1100
Washington, D.C. 20006
(202) 637-9800

Martin L. Stern
Lisa A. Leventhal
Preston Gates Ellis & Rouvelas
Meeds LLP
1735 New York Avenue, N.W., Suite 500
Washington, D.C. 20006
(202) 628-1700

Attorneys for Center for Democracy and Technology

Dated: May 20, 1998

SUMMARY

CALEA is but the latest chapter in the 30 year history of the federal wiretap laws, which have always sought to balance constitutional privacy protections and law enforcement interests. CALEA was intended to preserve a minimum law enforcement surveillance capability in the face of technological change. It was not intended to serve as the basis for mandated expansions in that capability. Rather, as was the case with earlier electronic surveillance legislation, Congress crafted a legislative scheme intended to balance the interests of law enforcement and privacy. That balance is reflected in the four assistance requirements set out in Section 103 of the Act.

The industry interim standard already violates the principle of balance by mandating a location tracking capability that Congress did not intend and by failing to require adequate privacy protection in packet networks of call content not authorized to be intercepted. Expansion of the industry standard as the FBI proposes would further upset the balance. Given Congress' particular concern with the expanding sensitivity of signaling information, it is unreasonable to conclude, as the FBI argues, that Congress would pass a law mandating further expansion in the richness of signaling data provided to law enforcement, under a mere pen register standard.

CALEA also went one step further than the previous wiretap statutes, affirmatively requiring the protection of privacy through technological means. Three of CALEA's four capability assistance requirements are intended to preserve law enforcement's surveillance capabilities. But the fourth requires carriers to ensure that their systems are capable of intercepting call content and call-identifying information "in a manner that protects . . . the privacy and security of communications and call-identifying information not authorized to be

intercepted." Section 103(a)(4) thus imposes on telecommunications carriers for the first time ever an affirmative obligation to protect the privacy of communications and call-identifying data not authorized to be intercepted. This has direct implications for the packet networks issue.

The Commission has a pivotal role in carrying forward Congress' historical balance between privacy and law enforcement into technologies that form the basis for a wide variety of new communications services. The two aspects of the industry interim standard that CDT's challenge highlights – wireless location information and packet network services – are technologies that are at the very heart of the digital communications revolution. Notably, it is with these two core technologies that CDT believes the industry interim standard gives law enforcement surveillance capabilities that intrude upon privacy contrary to Congress' intent. In this phase of the CALEA proceedings, the Commission is required by CALEA to ensure that the fundamental privacy/law enforcement balance is being adequately maintained for these cutting-edge technologies.

CALEA, however, does not prohibit these surveillance enhancing developments, if they come about as a result of business needs or market forces. If they are available, law enforcement can take advantage of them. But the government cannot mandate them through adoption of a standard that forms the CALEA "safe harbor" standard. It is the Commission's responsibility to narrowly interpret the CALEA requirements and prevent the imposition of capabilities that would upset the fundamental balance at the heart of the Act.

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance	)	CC Docket No. 97-213
For Law Enforcement Act	)	
	)	

COMMENTS OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY

Pursuant to the April 20, 1998 Public Notice, DA 98-762, ("Public Notice") in the captioned docket, the Center for Democracy and Technology ("CDT"), by its undersigned attorneys, hereby comments on the scope of the assistance capability requirements necessary to satisfy the obligations imposed by the Communications Assistance for Law Enforcement Act (the "Act" or "CALEA")[1] and the responsibility of the Commission to ensure that the Act is implemented in a way that protects the privacy of the American people.

As CDT will show, there are only three questions presently before the Commission and they are relatively narrow. First, does CALEA require wireless carriers to provide real-time location information? CDT will demonstrate that it does not. Second, does CALEA's requirement to "protect the privacy of communications not authorized to be intercepted" require carriers, where reasonably achievable, to separate addressing information from message content

---

[1] Pub. L. No. 103-414, 108 Stat. 4279 (1994), codified at 47 U.S.C. §§ 1001-1010 and in various sections of Title 18 and Title 47.

in packet networks? CDT will show that it does. And third, can a mandate for the FBI's punch list items be found in the language or legislative history of Section 103 of the Act? CDT will establish that no such mandate exists.

INTRODUCTION

CALEA is but the latest chapter in the 30 year history of the federal wiretap laws, which have always sought to balance constitutional privacy protections and law enforcement interests. CALEA was intended to preserve a minimum law enforcement surveillance capability in the face of technological change. It was not intended to serve as the basis for mandated expansions in that capability. It was enacted by Congress in response to FBI claims that new technologies would soon make it "virtually impossible" to carry out wiretaps. In the words of FBI Director Freeh, CALEA was intended to preserve the electronic surveillance capability "as it has existed since 1968."

Since 1968, the electronic surveillance capability has always been subject to limitations, both technological and legal. In 1968, and again in 1994 with CALEA, the question for Congress was whether wiretapping should be available to law enforcement at all. Congress in both cases decided that the technique should be available, but it crafted a legislative scheme intended to balance the interests of law enforcement and privacy.

The industry interim standard already violates the principle of balance by mandating a location tracking capability that Congress did not intend and by failing to require adequate privacy protection in packet networks of call content not authorized to be intercepted. Expansion of the industry standard as the FBI proposes would further upset the balance. Given Congress' consistent concerns with the growing intrusiveness of technology, it is impossible to conclude

that Congress intended CALEA to expand the surveillance capabilities of telecommunications technology yet further, as the DOJ and FBI now contend.

As Congress has seen the surveillance power of technology grow, it has become especially concerned about the increasingly detailed and revealing nature of transactional or signaling data associated with communications. This concern has grown, from 1968, when government access to signaling data was unregulated, through 1986, when Congress first established statutory rules for access to signaling data, to CALEA, when concerns with signaling information were a central focus of privacy objections to initial versions of the Act. Given Congress' particular concern with the expanding sensitivity of signaling information, it is unreasonable to conclude, as the FBI argues, that Congress would pass a law mandating further expansion in the richness of signaling data provided to law enforcement, under a mere pen register standard.

CALEA went one step further than the previous wiretap statutes, affirmatively requiring the protection of privacy through technological means. Three of CALEA's four capability assistance requirements are intended to preserve law enforcement's surveillance capabilities, but the fourth also mandates protection of privacy. Under Section 103(a)(4), carriers are required to ensure that their systems are capable of intercepting call content and call-identifying information "in a manner that protects . . . the privacy and security of communications and call-identifying information not authorized to be intercepted . . . ."[2] Section 103(a)(4) imposes on telecommunications carriers for the first time ever an affirmative obligation to protect the privacy

[2] 47 U.S.C.§ 1002(a)(4) (emphasis added)

of communications and call-identifying data not authorized to be intercepted. This has direct implications for the packet network issue.

The Commission has a pivotal role in carrying forward Congress' historical balance between privacy and law enforcement into technologies that form the basis for a wide variety of new communications services. The two aspects of the industry interim standard that CDT's challenge highlights – wireless location information and packet network services – are technologies that are at the very heart of the digital communications revolution. In the case of wireless services, tens of millions of Americans rely on cellular phones and PCS devices for personal and professional communications on a daily basis. The Internet, with its highly efficient packet-based architecture, is credited as the sine qua non of the information revolution and has expanded commercial, political, and educational opportunities for individuals in the United States and around the world.

Notably, it is with these two core technologies that CDT believes the industry interim standard gives law enforcement surveillance capabilities that intrude upon privacy contrary to Congress' intent. In this phase of the CALEA proceedings, the Commission is required by the statute to ensure that the fundamental privacy/law enforcement balance originally struck in 1968 is being adequately maintained for these cutting-edge technologies.

The Commission need not deny law enforcement any advantages of the new technology: it must only recognize that CALEA was intended to preserve a minimum surveillance capability and define what that capability is. To properly interpret CALEA, it is necessary to distinguish between what the statute requires and what law enforcement may take advantage of. CALEA mandated a minimum national baseline for law enforcement surveillance. CALEA cannot be

used by the government to require more than the minimum required by the four capability assistance requirements of Section 103(a)(1) - (4).

However, regardless of CALEA, there have been certain expansions in surveillance capability in recent years that came about as a result of business needs or market-driven developments. Location information in wireless systems is one such capability. In the future, there will be others. CALEA does not prohibit these surveillance enhancing developments, if they come about as a result of business needs or market forces. If they are available, law enforcement can take advantage of them. But the government cannot mandate them through adoption of a standard that forms the CALEA "safe harbor" standard. It is the Commission's responsibility to narrowly interpret the CALEA requirements and prevent the imposition of capabilities that would upset the fundamental balance at the heart of the Act.

DISCUSSION

I. THE COMMISSION'S ROLE IN THE IMPLEMENTATION OF CALEA

The CALEA framework seeks to balance three important policy interests:

> (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.[3]

Given these significant countervailing concerns, Congress did not seek to mandate the inclusion in the nation's telecommunications network of solutions to each and every complication that law enforcement might face when conducting its surveillance activities. Rather, the provisions of CALEA seek to strike the balance between "the legitimate needs of law enforcement and the constitutionally guaranteed rights of privacy of the individual."[4]

Balancing these interests, as described in the Act's legislative history, CALEA sets a floor on the surveillance assistance capabilities that carriers must build into their networks. Thus the Act mandates that carriers include *certain enumerated and limited* surveillance capabilities – the four items specified in Section 103 of the Act.[5] At the same time, CALEA serves as a ceiling on the surveillance assistance capabilities that carriers *must* build into their networks, for to

---

[3] *In the Matter of Communications Assistance for Law Enforcement Act*, 13 FCC Rcd. 3149, ¶ 5 (1997)(citing H.R. Rep. No. 103-827, pt. 1, at 13 (1994)).

[4] 140 Cong. Rec. H10773, H10780 (daily ed. Oct. 4, 1994)(statement of Rep. Markey).

[5] The Act also provides that carriers must comply with Section 103's four requirements within four years from the date of enactment, which is October 25, 1998. 47 U.S.C. § 1001(b). The October 1998 compliance date is the subject of the first round of comments submitted to the Commission, where CDT, telecommunications carriers and manufacturers all stated that compliance would be impossible by this date and urged the Commission to grant an industry-wide extension.

require anything more would tilt the critical balance that CALEA struck among privacy, law enforcement, and technological concerns.

CALEA contemplates that if a carrier or manufacturer fails to build the features required by Section 103 into its networks, the Attorney General may bring a civil action in U.S. District Court, seeking an order requiring that the carrier comply with the Act.[6] Such an order, however, cannot go beyond the limited requirements of Section 103, which operate as a bar on the surveillance assistance capabilities that may be imposed on carriers and their suppliers through a CALEA enforcement proceeding.[7]

At the same time, to provide carriers and manufacturers with an appropriate degree of certainty to avoid such enforcement actions, and to ensure CALEA's effective implementation on an industry-wide basis, Congress also established a consultative standards-setting process.[8] Under this process, industry, in consultation with law enforcement, may establish an industry-wide standard designed to ensure compliance with the four minimum assistance capabilities required by Section 103 of the Act. Such a standard would then serve as a "safe harbor," immunizing carriers and manufacturers in compliance with the standard from Section 108 enforcement actions.[9]

---

[6] The order may also direct that the carrier's equipment supplier provides modifications that would allow the carrier to comply. A similar order may be issued by a court issuing a surveillance order. 18 U.S.C. § 2522(a), (b).

[7] 47 U.S.C. § 1007(a).

[8] *See* 47 U.S.C. § 1006(a).

[9] *Id.* However, the absence of an industry-wide standard does not relieve carriers and manufacturers of their obligations under Section 103 of the Act. 47 U.S.C. § 1006(a)(3). Accordingly, an industry standard is critical if case-by-case, mass adjudications on what the Act requires are to be avoided.

Yet, even under this safe harbor procedure, industry and law enforcement are not the final arbiters of what CALEA requires. Rather, that is a responsibility that Congress has placed squarely on this Commission.[10] Thus, where, as here, a government agency or any other person files a petition alleging that the industry standard is deficient, it is the duty of this Commission "to establish, by rule, [the] technical requirements or standards" that CALEA requires.[11]

The Act directs the Commission, in establishing the CALEA standard, to ensure that the Commission's safe harbor not only serves to "meet the assistance capability requirements of Section 103 by cost-effective methods," but that it serves to "protect the privacy and security of communications not authorized to be intercepted."[12] Taken together, the five factors that the Commission must account for in Section 107(b) preclude the Commission from mandating a standard that falls outside the scope of the Act. In this manner, Congress ensured that a Commission-established safe harbor would preserve the critical balance between privacy concerns and law enforcement that formed the basis for Section 103.

Accordingly, the Commission's role in this proceeding is to preserve both the floor and the ceiling of the Act, as mandated by Congress. As further discussed below, Section 103 serves as CALEA's floor, providing for nationwide availability of only certain minimum assistance features. However, Section 103 also serves as CALEA's ceiling, reflecting a balance of technology, cost and privacy concerns with law enforcement interests, in providing that the CALEA standard must *meet but cannot exceed* the Act's minimum capability requirements. Section 103 thus stands as a bright-line boundary to the assistance capabilities that the industry

---

[10] This responsibility is, of course, subject to appellate review.

[11] 47 U.S.C. § 1006(b).

can be compelled to provide. There is simply no lawful basis for this Commission to include features that go beyond that boundary in establishing under Section 107 what CALEA requires.

II. IN ESTABLISHING A CALEA STANDARD, THE COMMISSION MUST MAINTAIN THE HISTORICAL BALANCE BETWEEN LAW ENFORCEMENT AND PRIVACY CONCERNS

The history of wiretapping laws in the United States, up to and including the enactment of CALEA, exhibits a fundamental tension between law enforcement and privacy interests. While Congress has accepted law enforcement's assertions regarding the value and necessity of wiretapping, at the same time, Congress has been persistently troubled by the significant privacy intrusions caused by the government's surreptitious interception of telephone and other electronic communications. Consequently, Congress' overriding objective when enacting the nation's wiretapping statutes has always been to achieve an appropriate balance between privacy and law enforcement interests.[13] In enacting CALEA, Congress was guided by this very objective and clearly intended to preserve this critical balance.

A. Congress has Historically Sought to Balance Law Enforcement and Privacy Interests to Protect the Constitutional Right to Privacy

Over the 30 year history of the nation's wiretapping legislation, Congress has expressed its continued concern over the increasing intrusion of new technologies into the realm of personal privacy. This concern is reflected in each major addition to the wiretapping statutes, and without exception, every such enactment struck a balance between law enforcement interests on the one hand and privacy interests on the other. Moreover, the need to strike an appropriate balance

---

[12] *Id.*

[13] These interests have been joined more recently by a third interest, namely encouraging technological innovation and competition in the communications industry.

between these competing interests can also be found in Supreme Court cases that predated, and to some degree prompted, the adoption of the first federal wiretap law.

For example, in 1963, the Chief Justice of the Supreme Court warned of how "the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual; [and] that indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments . . . ."[14] Again, in 1967, the Supreme Court found, in *Berger v. New York*, 388 U.S. 41, 63 (1967), that "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices."

1. The 1968 Federal Wiretap Law

Due to these substantial privacy concerns, which were gaining critical attention in the early 1960s, the enactment of the nation's first comprehensive federal wiretap statute faced multiple obstacles prior to its adoption in 1968.[15] In fact, the first major obstacle was whether wiretapping should be allowed at all. In the years leading up to the enactment of Title III, Congress held numerous hearings that were highly critical of wiretapping.[16] The criticism was so great that widespread private and public concern was generated and, for the first time in Department of Justice history, the Attorney General (Ramsey Clark) opposed governmental wiretapping altogether. The Johnson Administration sent legislation to Congress to outlaw all governmental wiretapping, except for cases involving national security. Only after considerable controversy was Title III passed as part of the Omnibus Crime Control and Safe Streets Act,

---

[14] *Lopez v. United States*, 373 U.S. 427, 441 (1963).

[15] This initial federal wiretap law is known as Title III, for it was Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

[16] In 1964, the Senate Judiciary Subcommittee, chaired by Senator Edward V. Long, began extensive hearings.

which was propelled to enactment by election year politics and the assassination of Robert F. Kennedy.

In deciding to authorize limited wiretapping capabilities pursuant to Title III, Congress agreed that changes in technology were eroding individual privacy rights. As evidenced by the Report of the Senate Judiciary Committee on Title III, "[t]he tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, privacy of communication is seriously jeopardized by these techniques of surveillance."[17]

Accordingly, Congress stated that "Title III has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized."[18] The Supreme Court, in its decision upholding Title III, found that "the protection of privacy was an overriding congressional concern."[19]

2. The Electronic Communications Privacy Act

Once again, in 1986, with the enactment of the Electronic Communications Privacy Act (ECPA), Congress took notice of the ever-increasing ability of technology to intrude upon personal privacy. ECPA extended Title III to wireless and non-voice communications and

---

[17] S. Rep. No. 1097, at 67 (1968).

[18] *Id.* at 66. Indeed, in recognition of the uniquely intrusive aspects of wiretapping, Congress imposed privacy protections in Title III that actually went beyond those required by the Fourth Amendment. For example, Congress limited the use of wiretapping to a prescribed list of more serious crimes. In addition, Title III required law enforcement to show that other Fourth Amendment techniques had been tried and were unsuccessful or would not be successful. Moreover, Title III required special high level Department of Justice approval to apply for a surveillance order.

established rules for law enforcement's use of pen registers and trap and trace devices. Pursuant to its enactment, Congress warned of the new threats posed by advances in technology:

> These tremendous advances in telecommunications and computer technologies have carried with them comparable technological advances in surveillance devices and techniques. *** Most importantly, the law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.[20]

ECPA did not signal the end of Congress' concern with the growing intrusiveness of technology. In August 1990, Senator Patrick J. Leahy, Chairman of the Senate Judiciary Subcommittee on Technology and the Law, hosted a hearing that focused on Caller ID technology. At that hearing, Senator Leahy, who was one of the leading sponsors of ECPA, and who would become one of the two primary sponsors of CALEA, concluded that ECPA needed to be reviewed in light of various significant developments in the area of communications technology, to ensure that the privacy protections within the statute had not been mooted by these new technologies.[21]

Consequently, Senator Leahy appointed a private sector task force to study ways in which ECPA might have been superseded by emerging technologies. The task force concluded that "five years after ECPA was enacted, a new array of technologies, which were only on the

---

[19] *Gelbard v. United States*, 408 U.S. 41, 48 (1972).

[20] S. Rep. No. 99-541, at 3, 5 (1986).

[21] See Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103d Cong., S. Hrg. 103-1022 (1994) ("Hearings"), at 179.

drawing board in 1986, are in the process of being deployed" and that these technologies "are challenging the existing statutory scheme for communications privacy."[22]

3. The Communications Assistance for Law Enforcement Act

Given this historical context, when Congress began considering the concerns voiced by law enforcement regarding the potential loss of surveillance capabilities due to the advancement of technology, it had already received ample evidence that these new technologies were in some ways enhancing the government's surveillance capabilities at the expense of protected privacy rights.[23] In their report on CALEA, the House and Senate Judiciary Committees specifically cited the report of Leahy's task force, noting, with concern, that "as the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance authority is clearly defined and appropriately limited."[24] The Committees warned of the "ever increasing opportunities for loss of privacy."[25]

Accordingly, when enacting CALEA, Congress reaffirmed that, "[f]or the past quarter century, the law of this nation regarding electronic surveillance has sought to balance the interests of privacy and law enforcement."[26] Clearly, CALEA was intended to preserve this important balance.

---

[22] *Id.* at 180.

[23] In fact, the Leahy task force report was incorporated into the hearing record for CALEA. *Id.* at 179.

[24] H.R. Rep. No. 103-827, pt.1, at 17 (1994)("House Report"). The Senate Judiciary Committee report is identical to the House Report being cited. S. Rep. No. 103-402 (1994). No other committees filed reports. Thus, although some sections of the legislation changed after the Judiciary Committees acted, the Judiciary Committee reports remain the best legislative history. Many provisions ultimately enacted were unchanged from the version reported by these Committees.

[25] House Report at 12.

[26] *Id.* at 11.

In addition to this historical background, the hearings on CALEA included specific testimony on the growing threat of electronic surveillance and the need to balance the competing interests of law enforcement and privacy. For instance, Jerry Berman, representing the Electronic Frontier Foundation at the time (he now serves as the Executive Director of CDT), opposed earlier drafts of CALEA because they did not adequately address the growing intrusiveness of new technologies. Later, when the legislation had been redrafted and narrowed, Berman praised its sponsors for "recognizing that technology is a two way street" and that the other side of the technology street is that when technology advances, privacy can also be impaired and undermined and eroded. This legislation, unlike previous drafts, as the FBI Director has pointed out, deals with some of those privacy problems that have been created by the evolving technology . . . .[27]

The FBI's proposed reading of CALEA would have this Commission ignore Congress' longstanding and consistent concern with the impact of electronic surveillance on fundamental privacy interests. Indeed, the FBI has urged the Commission to turn this history, as well as well-established constitutional privacy principles, on their heads, arguing that public safety and national security should now be the *paramount* considerations in the Commission's interpretation of CALEA.[28] It is this Commission's responsibility to preserve this historical balance by refusing to adopt this one-sided and erroneous view of the Act.

---

[27] Hearings at 158.

[28] In its comments in the related proceeding on CALEA security, the FBI incorrectly states that "[t]hese goals are to be achieved through whatever technical modifications are necessary." FBI Comments at ¶ 18. The FBI also incorrectly states that CALEA requires carriers offering calling features "to make all necessary network modifications to comply with CALEA." FBI Comments at ¶ 30. To the contrary, CALEA only requires carriers to make changes that are reasonably achievable and also makes clear that law enforcement cannot require carriers to build additional assistance requirements into their telecommunications networks. Indeed, Section 103(b)

In fact, not only has Congress sought to preserve an appropriate balance in CALEA, in the final analysis, it has placed privacy interests in front of law enforcement. During the CALEA hearings, Senator Arlen Specter stated that "[w]hen the crunch comes, we have always chosen privacy as the superior value in our country, and I think that has to be maintained."[29] The FBI's approach to CALEA would require the exact opposite of what Congress intended.

B. CALEA Was Not Intended to Provide a 100 Percent Solution to the Demands of Law Enforcement

Throughout this proceeding, the FBI has sought to create the impression that CALEA mandates a 100 percent solution to the difficulties it faces when conducting surveillance activities. The FBI has insisted on identifying *all* of the permutations an interception might take, *all* of the contingencies that could occur, and *all* of the bits of electronic information that it believes would be useful to have. Then, the FBI has tried to mandate in the CALEA standard the inclusion of features to address each and every one of these items. Consequently, while the FBI originally claimed that it was concerned with the total loss of wiretapping capabilities, due to the emergence of new technologies, and that it was only interested in preserving the "status quo," the FBI's most recent actions contravene its earlier representations as to the purpose and scope of CALEA.

The FBI began pushing for adoption of digital telephony legislation in the early 1990s because, as then FBI Director William Sessions stated, new technologies would soon make it

---

specifically states that CALEA does not authorize any law enforcement agency "to require any specific design" of telecommunications equipment, facilities or services. 47 U.S.C. § 1002(b)(1)(a).

[29] Hearings at 82.

"virtually impossible to capture criminal conversations."[30] The Clinton Administration's proposal for digital telephony legislation used the same language, arguing that legislation was necessary to prevent the virtually total loss of the ability to carry out wiretaps.

> The Problem: When in widespread use, [advanced telecommunications] technologies will make it virtually impossible for federal law enforcement agencies to use court-approved electronic surveillance.
>
> The Answer: Congress must enact legislation requiring that the new technologies contain capabilities allowing the government to continue using this invaluable tool to safeguard the United States.[31]

Furthermore, in 1994, FBI Director Louis Freeh appeared before Congress in support of the new legislation, arguing that the advancement of technology, if unaddressed by legislation, would result in a de facto "repeal" of Title III.[32] Freeh also claimed that telephone company executives were telling him that, unless Congress acted quickly to pass legislation, carriers would "not be able to service" the FBI's court orders for surveillance information.[33] Finally, the General Accounting Office also conducted an inquiry and concluded in similar terms that the ability to wiretap was "slowly vanishing."[34]

---

[30] "Advances in telecommunications technology promise to *deprive* Federal, state and local law enforcement officers and the public of the incalculable benefits that can be obtained only by court authorized wiretapping.***As in 1968, [Congress] must decide if law enforcement should have this valuable tool available." William S. Sessions, *Keeping an Ear on Crime: The FBI Needs Industry's Help*, N.Y. Times, Mar. 27, 1992, at A35 (emphasis added).

[31] Hearings at 259.

[32] Freeh stated that "[t]he purpose of this legislation, quite simply, is to maintain technological capabilities commensurate with existing statutory authority -- that is, to prevent advanced telecommunications technology from repealing, de facto, statutory authority now existing and conferred to us by the Congress." *Id.* at 7.

[33] *Id.* at 9.

[34] *Id.* at 127.

Congress was troubled by this impending loss of the wiretapping capability and, thus, it sought to preserve the status quo, as requested by the FBI, with the adoption of CALEA. Congress did not, however, attempt to create a 100 percent solution to each and every difficulty posed by the new technologies. Even the FBI acknowledged that CALEA was intended as a "stay-even proposition," preserving the FBI's "current access,"[35] and not as a directive authorizing "totally ubiquitous or penetrating" compliance requiring every piece of a carrier's network to meet the Act's requirements.[36]

Now, however, the FBI is divorcing itself from the rational position that it advocated when CALEA was adopted. Now the FBI is demanding that CALEA is much more than the mere preservation of the status quo, much more than a continuing balance of all competing interests. The FBI is now claiming that CALEA mandates a 100 percent solution to be imposed at the expense of all other concerns. The Commission must not accept, however, the FBI's post hoc characterization of CALEA, as it flatly contradicts the plain language and legislative history of the Act, as well as the FBI's own pronouncements as to what the Act would require and what it was intended to achieve. CALEA requires four minimum surveillance capabilities to be built into the networks of telecommunications carriers, no more and no less.

---

[35] *FBI Oversight and Authorization, Fiscal Year 1993*, Hearings Before The Subcomm. on Civil and Constitutional Rights of the House Judiciary Committee, 102nd Cong., 2d Sess., 9, 13, 49, 78 (1992).

[36] Hearings at 203. Further indication that Freeh was not striving for a 100 percent solution can be found in his recognition that a number of constraints limited the FBI's abilities under the statute. Freeh stated that, if sufficient funds were not appropriated, then law enforcement would be satisfied with a partial solution: "I would still be in a better place if I could have access to half of the criminal conversations than none of the criminal conversations." *Id.* at 197. Freeh also admitted that some surveillance targets would surely take steps to evade detection and that the legislation could not prevent such evasion. *Id.* He admitted that there would be technological impediments to surveillance: "There is always going to be and perhaps increasing because of the technology developments, a range of criminal activity and a particular type of criminal actor who will be immune from the best-designed and best-built system." *Id.* at 200.

Accordingly, CDT has petitioned the Commission to intervene in the establishment of a CALEA standard to preserve the longstanding balance between law enforcement and privacy interests. The industry interim standard already violates this balance by mandating a location tracking capability that Congress did not intend to be included within the Act, and by failing to require adequate privacy protections in packet networks. Moreover, expansion of the industry standard as the FBI proposes would further upset the balance.

III. THE COMMISSION MAY NOT ESTABLISH A CALEA STANDARD THAT INCLUDES ITEMS OUTSIDE THE SCOPE OF OR OTHERWISE PROHIBITED BY THE ACT'S MINIMUM CAPABILITY REQUIREMENTS

The Commission's task in this proceeding is, at bottom, a narrow one. Essentially, it must "establish by rule, technical requirements or standards" that *"meet* the assistance capability requirements of section 103," taking into consideration the privacy, cost, and other factors set forth in Section 107(b). At bottom, then, for a capability to be included in the Commission-approved standard, it must be required by one of the four requirements of Section 103. However, as will be seen, neither the wireless location information standard nor any of the items on the FBI's punch list is mandated by Section 103, and are in fact outside its scope. For these reasons, none of these items may be lawfully included in the resolution of the CALEA standard ultimately adopted by the Commission in this proceeding. Conversely, the standard's treatment of packet networks does not adequately meet the privacy protection requirement of subsection (a)(4) of Section 103.

A. "Call-Identifying Information" is a Narrow Concept and Does Not Justify Capabilities that the FBI Seeks to Require in the Standard

The call-identifying provision of Section 103 requires telecommunications carriers to ensure that their equipment, facilities or services "are capable of expeditiously isolating and

enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier."[37] The FBI tries to significantly expand the meaning of the term "call-identifying information" to require inclusion in the CALEA mandate of a wireless location function, as well as a number of items on the FBI punchlist.

The plain language of Section 103(a)(2), as well as its legislative history, demonstrates that "call-identifying information" is a precisely defined concept that encompasses only the numbers identifying the calling party, the called party and the duration of a call. Specifically, the Act defines "call-identifying information" as the "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier."[38] The detailed description of "call-identifying information" contained in the section-by-section analysis in the Committee Report leaves little doubt as to the term's meaning:

> The term 'call-identifying information' means the dialing or signaling information generated that identifies the origin and destination or [sic] a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization. For voice communications, this information is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted for the purpose of routing calls through the telecommunications carrier's network. In pen register investigations, these pulses, tones, or messages identify the numbers dialed from the facility that is the subject of the court order or other lawful authorization. In trap and trace investigations, these are the incoming pulses, tones, or messages which identify the originating number of the facility from which

[37] 47 U.S.C. § 1002(a)(2).

[38] 47 U.S.C. § 1001(2).